



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,017	03/18/2004	Wilson Sing-Hei So	36992.00107 (HAL 265)	7773

44955 7590 04/28/2008
SQUIRE, SANDERS & DEMPSEY L.L.P.
1 MARITIME PLAZA, SUITE 300
SAN FRANCISCO, CA 94111

EXAMINER

JOHNS, CHRISTOPHER C

ART UNIT

PAPER NUMBER

3621

MAIL DATE

DELIVERY MODE

04/28/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/805,017

Applicant(s)

SO ET AL.

Examiner

Christopher C. Johns

Art Unit

3621

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 February 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6, 8-16, 18 and 19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-16, 18 and 19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Acknowledgements

1. Claims 7, 17, and 20 were cancelled.
2. Claims 1 and 12 were amended.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 3-6, 8-12, 14-16, 18, and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 6,105,008 (hereafter "Davis").
5. As per claims 1 and 12, Davis teaches:
6. first site coupled to a network (figure 10, reference number 504; Abstract);
7. terminal coupled to network for performing first portion of a transaction with first site (figure 10, reference numbers 502, 504, 506, 508, 510, 512);
8. second site coupled to the network for performing second portion of the transaction that requires personal data, second site transmits to the terminal via the network a certificate for verifying the identity of the second site (figure 10, reference numbers 512, 518);
9. secure device coupled to the terminal (figure 10, reference number 502; figure 4, reference numbers 218, 220), containing an encrypted version of the personal data and

Art Unit: 3621

a first key for decrypting the encrypted personal data, and provides the terminal with the encrypted personal data and the first key (column 19, lines 52-67; figure 5, reference numbers 312, 314, 326; figure 6, reference number 314a);

10. terminal having logic for decrypting the encrypted personal data using the first key, logic for re-encrypting the decrypted personal data with a second key, logic for transmitting the re-encrypted personal data to the second site via the network (it is inherent in Internet transactions to encrypt and decrypt data, because security is an objective over a network such as the Internet. Additionally, see generally column 19, lines 33-47; column 21, lines 6-8);

11. second site having logic for decrypting the re-encrypted personal data and logic for using the personal data to complete the second portion of the transaction (column 29, lines 9-19);

12. secure device provides the terminal with the encrypted personal data prior to and separately from the first key (the device and terminal share the DES key, see column 19, lines 59-60, where the key is referred to as a "Shared key". Furthermore, see column 19, lines 55-57: "Through a **prior business arrangement**, both of the servers have arranged to share this unique key to add security to the transaction". Additionally, see figure 9, reference number 402).

13. As per claims 3-6, 8-11, 14-16, 18, and 19, Davis discloses:

14. communication between the terminal and the secure device and between the terminal and second site are encrypted with one or more symmetric keys (column 19, lines 52-67, *et seq*);
15. personal data includes at least one of credit card information (Abstract: the smart card can be used for "payment of goods and/or services purchased on-line over the Internet"; also column 1, lines 30-35 – "may be programmed with various types of functionality, such as a stored-value application, credit/debit...");
16. list containing information for authenticating the certificate of the second site transmitted from the first site to the terminal via the network prior to the receipt of the certificate by the terminal (figure 11A, reference number 606: allows client terminal to understand where to go for payment (part of the information sent is the IP address of the payment server), as well as the identities of the transaction and merchant using identifiers (allowing for further verification of the validity of the server));
17. transaction comprises a commercial transaction and the first site comprises an e-commerce site (Abstract: "smart card for payment of goods and/or services purchased on-line over the Internet");
18. second key comprises a public key associated with the second site (column 19, lines 52-67, *et seq*);
19. second certificate associated with the terminal is provided to the second device to authenticate the terminal before the secure device provides to the terminal with the encrypted personal data and first key;

Art Unit: 3621

20. notification is transmitted from the second site to the first site via the network upon completion of the second portion of the transaction (figure 11C, reference numbers 634, 636, 638, 640);
21. secure device is detachably coupled to the terminal (figure 4 – note that both reference number 5 is inside reference number 210, and that reference number 220 is inside reference number 216).

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

23. Claims 2 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, in view of Official Notice.
24. As per claims 2 and 13, Davis does not explicitly disclose that the secure device includes a special region that, if tampered with, renders the secure device inoperable and thereby prevents access to the first key. The Examiner takes Official Notice that deactivating circuitry was old and well-known in the art because it allows for a way to keep private information secure to even the most determined attackers. It was old and well-known to those skilled in the art at the time of the invention to destroy information when the information was important and there was a significant impetus to keep it from being released. This solution provides a more secure system where data will not fall

into an attacker's hands. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ a mechanism to destroy circuitry upon an intrusion detection, because it would provide a more secure system where the first key would not be obtained. A person having ordinary skill in the art would understand this as an advantage, namely that an attacker would not be able to compromise the system because of a single card.

Response to Arguments

25. Applicant's arguments filed 15 February 2008 have been fully considered but they are not persuasive. Applicants' claim that Davis does not teach the secure device providing the terminal with the encrypted personal data prior to and separately from the first key. The DES algorithm, old and well-known to those skilled in the art at the time of the invention, involves a symmetric key. This means that both parties must have the same key – in fact, the key is established using previous transaction, as in column 19, lines 55-57.

Conclusion

26. **Examiner's Note:** Although Examiner has cited particular columns, line numbers and figures in the references as applied to the claims above for the convenience of the applicant(s), the specified citations are merely representative of the teaching of the prior art that are applied to specific limitations within the individual claim and other passages and figures may apply as well. It is respectfully requested that the applicant(s), in

Art Unit: 3621

preparing the response, fully consider the items of evidence in their entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

27. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

28. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is (571)270-3462. The examiner can normally be reached on Monday - Friday, 9 am to 5 pm.

30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3621

31. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher C Johns
Examiner
Art Unit 3621

CCJ

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621